

11.2
10.15

STAT



PREFACE

This brochure serves as a guide for preparing and submitting proposals for research support in mathematics or cryptology. Included is an overview of specific areas of interest, guidance and necessary requirements for preparation and submission of the proposal, and some general administrative information.

Authority for Publication:

NSA/CSS Directive 60-11
Grants and Cooperative Agreements for Research in Cryptology
Dated 6 August 1981

NATIONAL SECURITY AGENCY
MATHEMATICAL SCIENCES PROGRAM
(Formerly Program OCREAE)
Grants for Research in Mathematics and Cryptology

INTRODUCTION

In January 1987, Lieutenant General William E. Odom, Director of the National Security Agency, announced the expansion and redirection of Program OCREAE, NSA's grants program for research in cryptology and related areas. Spurred by the importance of mathematics to NSA in performing its mission and by the findings of the National Research Council report, *Renewing U. S. Mathematics* (the "David Report"), NSA decided that it must act decisively to help insure the strength and vitality of American mathematics. This action will include changing the focus of the NSA grants program almost exclusively to pure mathematics. Reflecting this new direction is a name change: from Program OCREAE to the NSA Mathematical Sciences Program.

Work was formerly supported by Program OCREAE in the loosely defined area of "cryptologic related research." Under its new direction, the NSA Mathematical Sciences Program will devote the bulk of its funding (perhaps 80-90%) to mathematics, and the remainder to cryptologic related research.

AREAS OF INTEREST

The NSA Mathematical Sciences Program is interested in supporting research in the following areas of pure mathematics: Algebra, Number Theory, Discrete Mathematics, Probability, and Statistics. Because of the universal applicability of these areas to cryptology, it is not necessary that this mathematical research have any immediate connection to cryptology. From time to time, research in certain areas may be stressed, and there will be support for some special projects in

mathematics, such as "special years" at universities. Researchers are encouraged to call the Program Director to find out about current areas of special emphasis.

NSA also supports research dealing with the design and analysis of cryptographic algorithms, particularly the theoretical foundations of cryptology. Researchers may submit proposals on any aspect of information security, but it should be noted that cryptographic protocols and hardware implementation of algorithms, while of great importance, are of marginal interest to the NSA Mathematical Sciences Program.

SELECTION CRITERIA

Grant awards will be made on the basis of several factors determining the scientific merit of the proposal, including : (1) the prospect that the research will lead to important discoveries; (2) the prospect that the research will produce innovations or significant improvements in investigative methods; (3) the investigator's scientific qualifications and accomplishments; (4) the investigator's demonstrated awareness of previous approaches to the problem. The NSA Mathematical Sciences Program attempts to have a wide geographic and institutional distribution of support, and NSA encourages proposals from traditionally underrepresented groups.

TECHNICAL EVALUATION

A panel of the Board on Mathematical Sciences of the National Research Council provides an independent peer review of all mathematics research proposals submitted to the NSA Mathematical Sciences Program. Proposals for research in cryptology are reviewed by an internal NSA review board.

DISCLOSURE OF INFORMATION

Although it is the intent of the NSA Mathematical Sciences Program that the research it supports will produce only unclassified

results, it should be recognized that research in cryptologic areas may produce information whose disclosure could harm U.S. national security. In order to deal with this possibility, the following disclosure policy is incorporated in each NSA grant:

"It is expected that the recipient may make formal public disclosure of the scientific and technical information resulting from this agreement (e.g., release articles for appropriate professional publications or present papers at scientific meetings or symposia). Such disclosure is authorized as long as a copy of the article, paper, report, etc., shall be provided to the Government, preferably in advance, but at least concurrent with public disclosure. It is also understood and agreed that the recipient may utilize the scientific and technical information resulting from this work in consulting or discussing this and related information with other qualified individuals or groups of individuals, where appropriate, for furthering research. In the event that the researcher believes information generated during the research may require classification, the researcher shall notify NSA and request that the information be reviewed for classification prior to further dissemination."

WHO MAY SUBMIT

Awards will be made *only* to nonprofit institutions. Such awards will be based on a formal proposal submitted by an organization on behalf of the principal investigator(s). It is NSA's intent to support American mathematics; *therefore, for mathematics grants the principal investigator and all research personnel must be U. S. citizens.* To be eligible for an award the organization must have submitted a Certificate of Assurance or Compliance with Title VI of the Civil Rights Act of 1964 and be constantly in compliance with the Act.

WHEN TO SUBMIT

There are two deadlines for grant applications:

★ 1 November for grants to begin the following summer or fall,

★ 1 May for grants to begin the following winter or spring.

A proposal should give the preferred starting date, taking into account that technical review, negotiation, and award normally take nine (9) months.

WHAT TO SUBMIT

No specific form is now required, though applicants are cautioned to include all necessary data (outlined below). An original and *seven (7) copies* of the proposal must be submitted.

Name and Address of Organization - Proposals should be submitted on the institution's letterhead stationery giving the legal name and address of the organization. The names and telephone numbers of technical and business personnel should be provided. The home telephone number of the principal investigators is useful.

Organizational Endorsement and Approval - At least one (1) copy of the proposal must carry the original signatures of the principal investigator(s), the department head, and an official authorized to sign for the institution. All copies should indicate who signed the original proposal, giving the official title in each case.

Confirmation of Indirect Rates - Include either the name, address, and phone number of the federal government audit agency that will confirm the indirect rates proposed in the budget, or a copy of the latest rate agreement (usually with the Department of Health and Human Services) covering at least the requested starting date of the grant.

Title of Proposed Research - The title of the proposed research should be brief but properly descriptive and should use keywords suitable for indexing and retrieval. It should avoid symbols, alphabetical letters, and mathematical or scientific notation.

Time Period – The length of time for which support is requested should be consistent with the nature and complexity of the proposed research. Multi-year grants shall be funded on an annual basis.

Summary – A one page summary of the work being proposed must be the first section of the proposal. The summary should be self-contained, should avoid symbols, and should be expressed, as far as possible, in language understandable to a scientifically literate reader.

Description of Proposed Research – Submit a detailed description of the research to be undertaken, its objectives and approach, and its relationship to the state of knowledge in the field and to comparable work in progress elsewhere.

Personnel – The qualifications of the principal investigator and the time the principal investigator and other senior professional personnel will devote to the research are important factors in the selection of proposals for NSA support. *For mathematics grants the principal investigator and all research personnel must be American citizens.* The information* below will help in evaluating the proposal.

- 1) For the principal investigator and the senior staff, include:
 - (a) a short biography and a list of major publications;
 - (b) information on other commitments of time, such as sabbatical or extended leave; and
 - (c) proportion of time to be devoted to this and other research.
- 2) Indicate if the principal investigator or other key personnel have applied to or receive support from other agencies for this or other research.

*This information about an individual is subject to the requirements of the Privacy Act of 1974 (Public Law 93-579). The information is requested under the authority of Title 10, US Code Sections 2358 and 8012, and Title 42, US Code, Sections 1891-93. The principal purpose and routine use of the requested information are for the evaluation of the qualifications of those persons who will perform the proposed research. Disclosure of the requested information is voluntary, but failure to provide such will prevent evaluation of the proposal.

- 3) List the number of postdoctoral, student, or other research assistants and their scientific training and experience.
- 4) Give the names and association with the project of other technical personnel who will be working on the research.

Bibliography – Include a bibliography and a list of pertinent literature citations. When relevant to the proposed research or indicative of the applicant's ability, include summaries of these and preprints or reprints of research not yet available in readily accessible journals.

Facilities and Equipment Available – Facilities available for the research should be described as well as other facilities or equipment the organization intends to acquire under the proposed effort. Such equipment must be reasonably justified by the description of the work.

Proprietary Data – Identify any proprietary data within the proposal that is to be used for evaluation purposes only.

Other Sponsors – Provide the names of other parties that have funded, are funding, or have been asked to fund the proposed research.

FINANCIAL SUPPORT

NSA will cooperate with other granting agencies to provide appropriate levels of support for research proposals. A typical research grant supported by the NSA Mathematical Sciences Program for a single investigator might include funding for the following items:

- up to 2.5 months of salary support annually for the principal investigator (summer *or* academic year);
- 50% support (salary and tuition) for 1 or 2 graduate students;
- 50% support for a postdoctoral research assistant;
- support for a regional mathematics workshop;
- 1 trip to the annual program review in Baltimore;
- computer support *required* by the research;
- \$2,500 in other expenses for travel, supplies, etc.

Creative approaches to financial support are encouraged, but should be discussed with the Program Director before a proposal is submitted.

An estimate of the total cost of the research project with a breakdown of funds by category and year must accompany the proposal. A sample cost estimate is included at the back of this brochure for guidance in preparing that estimate. If a portion of the total research cost is to be furnished by the offerer, the source and amount should be set forth separately from that money requested from the Agency.

The cost principles of OMB Circular A-21 will be applicable to agreements with educational institutions and the cost principles of OMB Circular A-122 shall be applicable for nonprofit organizations. For projects of more than one (1) year duration, separate estimates are required for each year.

PAYMENTS

If advance payments are requested, please provide a suggested payment schedule. The requested schedule should include the dates invoices would be submitted and the amount (by dollars or percent of the grant) for each payment request.

JOINT SPONSORSHIP

Present or prospective joint sponsorship of any portion of the program outlined in the proposal should be disclosed in the proposal. Prior approval of all agencies must be secured for research to be undertaken under joint sponsorship.

GRANT ADMINISTRATION

The NSA Office of Contracting administers the non-technical aspects of grants. Further details, including *General Provisions for NSA Grants and Cooperative Agreements*, may be obtained from:

*National Security Agency
Office of Contracting
Attention: L431
Fort George G. Meade, Maryland 20755-6000*

FURTHER INFORMATION

Further information on grants is available by writing or calling:

Director
NSA Mathematical Sciences Program
National Security Agency
Attention: RMA
Ft. George G. Meade, MD 20755-6000

(301) 859-6438

STAT

SAMPLE COST ESTIMATE

| <i>1 June 198n through 30 June 198n+1</i> | <i>Agency Support</i> | <i>Cost Share</i> | <i>Total Cost</i> |
|---|---------------------------|-----------------------|-----------------------|
| 1. SALARIES & WAGES | | | |
| a. Principal Investigator - J. Q. Math | | | |
| Two month acad. yr. @ \$5,500*/mo. | \$ 5,500 | \$ 5,500 | \$ 11,000 |
| One month summer @ \$5,000/month | \$ 5,000 | | \$ 5,000 |
| *Assumes a 10% increase 1 July | | | |
| b. Postdoctoral Researcher - K. R. Math | | | |
| Full-time, 12 mos. @ \$3,000/mo. | \$18,000 | \$18,000 | \$ 36,000 |
| c. 1 Graduate Research Assistants | | | |
| Tuition @ \$3,500/semes. | | \$ 3,500 | \$ 3,500 |
| Half-time, 9 mos. @ \$500/mo. | \$ 4,500 | | \$ 4,500 |
| Full-time summer, 3 mos. @ \$1,000/mo. | \$ 3,000 | | \$ 3,000 |
| TOTAL SALARIES & WAGES | <u>\$36,000</u> | <u>\$27,000</u> | <u>\$ 63,000</u> |
| 2. EMPLOYEE BENEFITS | | | |
| 26.5% of regular faculty salaries | \$ 2,783 | \$ 1,457 | \$ 4,240 |
| 20.0% of visiting faculty salaries | \$ 3,600 | \$ 3,600 | \$ 7,200 |
| 16.0% of student salaries | \$ 1,200 | | \$ 1,200 |
| TOTAL EMPLOYEE BENEFITS | <u>\$ 7,583</u> | <u>\$ 5,057</u> | <u>\$ 12,640</u> |
| 3. COMPUTER COSTS | | | |
| (See justification in Note 1) | | | |
| 15 hrs. @ \$75/hr. | <u>\$ 1,125</u> | | <u>\$ 1,125</u> |
| 4. THREE DAY SUMMER WORKSHOP | | | |
| (Workshop details are in Note 2) | | | |
| University Support Services | | \$ 3,500 | \$ 3,500 |
| Three principal lecturers @\$500 ea. | \$ 1,500 | | \$ 1,500 |
| Secretarial support | \$ 1,000 | | \$ 1,000 |
| Student stipends, 12 @ \$150 | \$ 1,800 | | \$ 1,800 |
| Printing & Publicity | \$ 1,500 | | \$ 1,500 |
| TOTAL WORKSHOP COSTS | <u>\$ 5,800</u> | <u>\$ 3,500</u> | <u>\$ 9,300</u> |
| 5. PUBLICATION AND REPORT COSTS | | | |
| 10 pages @ \$50/page | <u>\$ 500</u> | | <u>\$ 500</u> |
| 6. OTHER DIRECT COSTS | | | |
| Telephone, photocopy, communications | <u>\$ 500</u> | | <u>\$ 500</u> |

7. TRAVEL

| | | | |
|---|-----------------|-----------------|------------------|
| 1 to West Coast for technical meeting \$450 travel plus 3 days @ \$150/day | \$ 900 | | \$ 900 |
| 2 to Baltimore for annual MSP review P.I. and student, \$350 travel plus 2 days @ \$125/day | \$ 1,200 | | \$ 1,200 |
| TOTAL TRAVEL | <u>\$ 2,100</u> | | <u>\$ 2,100</u> |
| TOTAL DIRECT COSTS | <u>\$53,608</u> | <u>\$35,557</u> | <u>\$ 89,165</u> |

8. INDIRECT COSTS

| | | | |
|--------------------------------|-----------------|-----------------|------------------|
| Current Provisional rate - 56% | | | |
| NSA support 56% × \$49,138 | \$30,020 | | \$ 30,020 |
| Cost share 56% × \$38,425 | | <u>\$19,912</u> | <u>\$ 19,912</u> |
| TOTAL ESTIMATED COSTS | <u>\$83,628</u> | <u>\$55,469</u> | <u>\$139,097</u> |



Mathematics and NSA . . . A Long-Term Partnership

Each year, some of the nation's leading mathematicians take on an extraordinary challenge—they go to work for the National Security Agency. NSA's Mathematical Sabbatical Program offers an opportunity to work on a short-term basis with the leading employer of mathematicians in the United States. And it offers a personal challenge as well: to develop one's skills in directions that would be impossible anywhere else.

The sabbaticals primarily involve cryptanalysis, a discipline highly dependent on superior math ability. Cryptanalysis requires

background, perspective and experience that cannot be learned overnight. History shows, however, that visiting mathematicians are quick learners and make a significant contribution in a short time. Other sabbatical work involves algebra, probability, statistics, number theory and discrete mathematics.

Questions you may have

Just what is the NSA?

The National Security Agency makes a vital contribution to an

informed and secure environment for our nation's policy-making. Established by presidential directive in 1952, it is the Department of Defense agency responsible for producing foreign intelligence information. It also safeguards our government's vital communications, and sets standards for computer security throughout the federal government. These missions require the use of the most advanced technologies and techniques, often years before their commercial use.

What is the NSA math environment like?

Mathematicians at NSA enjoy the type of dynamic environment that only the largest employer of mathematicians can offer. In addition to our own in-house publications, we offer: summer workshop programs, continuing colloquia, cooperative education programs and occasional meetings that provide opportunities to interact with mathematicians both within and outside the agency. NSA also awards grants for research in cryptology and related areas. Further, as a member of the NSA professional staff, you will have access to support services. For example, our computer services are available to assist you with research.

Will I still be able to publish my work?

Publishing is important to all serious mathematicians. NSA provides ample opportunity to inform your contemporaries of your work. The in-house publication, *Cryptologic Quarterly*, is one such forum. Because of the nature of the work, however, publications outside the NSA community must be cleared through our public information office. This is also true after you leave our employ, *but only for work directly related*

to your research at NSA. And of course, any classified techniques you are involved with cannot be reported.

How long do NSA sabbaticals last?

Mathematical sabbaticals can run from 9 to 24 months, and we are flexible regarding start dates.

What kind of compensation can I expect?

NSA will supplement mathematicians' University stipends to at least equal their regular monthly salary. You may choose either an allowance for moving expenses *or* a housing supplement.

How are sabbatical applicants screened?

Keep in mind that mathematical achievement is the main criterion for selection. The applicant must participate in a thorough and extensive screening process. In addition to psychological testing and interviewing, there is a polygraph exam, personnel interview, and interviews with senior mathematicians at NSA. Applicants will be given an opportunity to make presentations on their current research. A complete background investigation is also required.

How do I apply?

Those mathematicians interested must submit a U.S. Government application form (SF-171, available in campus placement offices), a curriculum vita, including a complete list of publications, and any other relevant information to:



**National
Security
Agency**

Director
NSA Mathematical Sabbatical
Program
ATTN: RMA
National Security Agency
Fort George G. Meade,
Maryland 20755-6000
*The application deadline is
August 1st. Call (301) 859-6438
for more information.*

An equal opportunity employer.
U.S. citizenship required for applicant and
immediate family members.

STAT



National
Security
Agency